Summer 2003

HOOSIER SAFETY

A Publication of
The Indiana State Emergency Management Agency
and Department of Fire and Building Services

JULY STORMS INUNDATE STATE -- FEDERAL DISASTER DECLARATION APPROVED BY PRESIDENT

Near record rainfall in early July resulted in widespread flooding throughout Indiana

Not all of the fireworks on the Fourth of July came from public displays or backyard celebrations this year. Nature put on a quite a show of its own, and that was just the beginning.

Severe storms continued on a daily basis for more than a week with rivers remaining above flood stage in parts of the state for much of the month. The flood fight included National Guard troops and Department of Corrections inmates sandbagging in Bluffton and Decatur. Many other state agencies did their part as well.

The human toll was high. Four deaths were reported and more than 4,500 claims for assistance had been filed at press time. Forty-one counties had been declared Presidential Disaster Areas. They are: Adams, Allen, Benton, Blackford, Boone, Carroll, Cass, Clinton, Delaware, Fountain, Grant, Hamilton, Hancock, Henry, Howard, Huntington, Jasper, Jay, Kosciusko, Madison, Marion, Miami, Montgomery, Noble, Pulaski, Randolph, Tippecanoe, Tipton, Union, Wabash, Warren, Wayne, Wells, White and Whitley.

I N S I D E

HIPAA

Health Insurance Portability and Accountability Act

The Office of Health and Human Services (HHS) created HIPAA, which affects the handling of Private Health Information (PHI), by Covered Entities (CE). HIPAA has four primary components - Transactions & Codesets, Privacy & Health information (the Privacy Rule), Security & Health Information, and Identifiers. This article, transcribed from a PowerPoint presentation created by Mr. Michael Sommerkamp, Legal Counsel for SEMA, will only address the Privacy Rule, which creates a national floor for privacy standards and became enforceable on April 14, 2003.

All EMS providers are strongly encouraged to consult with their attorneys and medical directors when drafting and implementing policies regarding HIPAA compliance, disclosures of PHI, and disclosure of PHI to law enforcement officers.

"The intent of the Privacy Rule is to give individuals basic rights regarding the use of their PHI. The Privacy Rule, however, should ***NEVER*** compromise patient care", according to Sommerkamp. He further stresses that "HIPAA should ***NEVER*** adversely affect the quality of patient care rendered or impede the ability of a health care provider to care for a patient."

First - Are You a Covered Entity?

A Covered Entity is a health plan, a health clearinghouse, or a health care provider, who electronically transmits health information for a transaction covered under HIPAA. Common transactions include eligibility inquiries, health claims and other billing matters done by you or *for your benefit* - so use of a 3rd party billing company does NOT exempt you from HIPPA. Yet, sending data to SEMA or NFIRS is NOT a covered transaction and, done alone, will not make you a CE. Even if you are not a Covered Entity, you would be wise to comply with HIPAA. To begin with, Medicare, as a general rule, will not pay claims that are not submitted electronically after October 16, 2003, unless a one-year waiver is sought and granted. Further, the public expects HIPAA's privacy standards and your potential jury pool in a privacy case brought under state law may judge you under the HIPAA yardstick.

Requirements of Covered Entities

Covered Entities must "**Protect PHI, which includes all individually identifiable health information regardless of whether it is in electronic form, paper, or oral communications**." Further, Covered Entities must:

- Designate a Privacy Official.
- Look for Leaks in their Privacy Policy.
- Conduct and document privacy training for their ENTIRE workforce.
- Develop an Authorization Form for the release of PHI.
- Develop a Notice of Privacy Practices.
- Understand the interaction of HIPAA and State Laws.
- Understand Patient Rights and associated requirements.
- Update employee policies and procedures
- Identify Business Associates and adopt a form contract.
- Put in place reasonable administrative, technical, and physical safeguards to protect PHI.

But most importantly, Covered Entities MUST know and live by "THE MINIMUM NECESSARY RULE" which states: When disclosure is allowed, ALWAYS disclose the MINIMUM PHI NECESSARY.

OH, BY THE WAY,

Patient Rights include the RIGHT to:

- Access their PHI.
- To REQUEST to amend their PHI.
- To place Restrictions on Use or Disclosure of their PHI.

See "HIPAA" page 3

"HIPAA" *from page 2*

- To Receive Alternative Communications.
- To Receive an Accounting of Unauthorized Disclosures.
- Additionally, patients are to be given a Notice of Privacy Practices.
- And the NPP has to tell them How to File a Complaint.

The Standard for Protecting PHI

Covered entities shall maintain *reasonable* and *appropriate* administrative, technical, and physical safeguards to ensure the integrity and confidentiality of the information (electronic, written, or spoken) and to protect against any *reasonably* anticipated threat or hazard to the security or integrity of the information; to protect against any unauthorized uses or disclosures of the information; and to otherwise to ensure compliance by officers & employees. While tremendous steps must be taken to protect patient information, HHS has stated that the use of encoded radio or electronic transmissions is NOT REQUIRED. Some common-sense steps towards protecting patient information can go a long way - these include:

- Maintain run sheets in a secured area and limit access.
- Add passwords to computers and networks that contain PHI.
- Add confidentiality statements on e-mails and faxes that contain PHI.
- And maintain the fax machine that receives PHI in a secure location and limit access.

While incidental disclosures can be made for treatment, a wise care provider will always use discretion and the most secure manner available to transmit PHI:

- If a patient name *must* be used when contacting the hospital, then use a cell phone if possible, as opposed to the radio.
- If others not involved in treatment are near, then whisper.
- Common sense and a team approach towards compliance can go a long way.

Beware of any use or discussion of PHI NOT specifically permitted in the Privacy Rule, such as discussing a run at the station, a Pizza Hut, a gym, a bar, or anyplace *other than Audit and Review*. Also beware of discussing "interesting" runs, famous patients, or even relatives or neighbors. These standards obviously cover the medics who produce your PHI, but they also cover billing agents and anyone else who handles or has access to your PHI. When unsure whether you should discuss a run, ask yourself if the disclosure was for the benefit of the patient AND that it was done with the utmost discretion.

Designate a Privacy Official

All Covered Entities must appoint a Privacy Officer who will then develop a Privacy Program and create procedures with the assistance of both the medical director and the attorney who would defend that provider against an action brought by the "HIPAA Police". While the Privacy Officer can have other duties, he or she must have the time and resources needed to fulfill the required HIPAA duties.

Who Is An Employee?

For the purpose of the Privacy Rule employees are volunteers, students, trainees, independent contractors, and anyone else under your control. This includes employees of other services who periodically respond in your vehicles.

Look for Leaks in Your Privacy Policy

Analyze how your service handles PHI and look for "Leaks" where PHI can seep through. Guarding PHI *HAS* to be an ongoing task for everyone: Students, EMTs, Billing Agents, the Privacy Officer, and Management. Remember, HIPAA covers electronic, written, and oral disclosures of PHI.

Develop an Authorization Form for the Release of PHI

Most EMS disclosures fall under the Treatment, Payment, and Health Care Operations (TPO) exemption, which means that pateint authorization is not required. Authorization is required for disclosures NOT otherwise authorized under the Privacy Rule.

See "HIPAA" page 4

"HIPAA" *from page 3*

One of the few situations where an EMS provider might need authorization to disclose PHI would be for marketing NOT conducted by the provider.

Notice of Privacy Practices, or NPP

Covered Entities must develop a compliant NPP. The NPP must be in plain language, which might require a Spanish NPP if you serve a Spanish-speaking community. Covered Entities must make a Good Faith attempt in non-emergency situations to both give a NPP to each patient or patient's representative **AND** to get a signed Acknowledgement of Receipt by each patient or patients representative. In Emergency Treatment Situations, the NPP must be given as soon as *practical*—which could mean to leave a copy at hospital, or to mail it with the bill. If a patient refuses a run you should make a good faith effort to both give the patient a NPP and to get her signature on the Acknowledgement of Receipt form, which could be added to the refusal form you now use. Services who maintain a web site MUST post their NPP on their site (Look for free examples of NPP on the internet). Keep in mind that the NPP has many technical requirements. Consult the Privacy Rule to ensure your chosen examples *themselves* comply with the Privacy Rule.

NPPS & Unemancipated Minors

The Privacy Rule does NOT address consent to treatment, so Indiana law regarding the ability of minors to consent (or to sign to refuse treatment) is unchanged. Just as a minor in Indiana is not deemed competent to refuse treatment, a minor is likely not deemed competent to accept a NPP or to sign for its acceptance. In descending order, the following may give consent for medical treatment for an unemancipated minor, which means that the following may also accept a NPP or may sign to accept a NPP for an unemancipated minor:

- A court-appointed guardian; (if none is available) then
- A parent or person acting *in loco parentis;* (which means "acting as a parent)(if neither is available) then
- An adult sibling; (if none of the preceding are available) then
- A law enforcement officer who believes the minor's condition is "seriously impaired or endangered".

Patient Rights

Patient Rights requirements are detailed and MUST be precisely followed. Most patient rights MUST be listed on the NPP. If a patient is not legally competent, then a patient representative may exercise that patient's rights. Patients must be allowed to access and copy their PHI within 30 days of their request to access and copy. Providers must make a good faith effort to give every patient a NPP *as soon as practical* and to get a Signature of Receipt from the patient. Patients have the right to *REQUEST* to amend records. Patients can request an accounting of unauthorized and non-routine disclosures of their PHI for up to 6 years, ***BUT***, only for dates ***after*** April 14, 2003. Finally, patients must be told on the NPP how to file a complaint.

Business Associates

Entities who perform services on your behalf and have access to your PHI are Business Associates. Your employees and other care providers are *not* Business Associates. As a general rule, individuals who ***create*** PHI are not Business Associates, while individuals who use your PHI are Business Associates. Potential Business Associates include: third party billing companies, outside claims consultants, outside medical directors, software vendors, computer consultants, and computer repair personnel.

HIPAA & State Laws

HIPAA preempts less stringent state privacy laws. In addition to HIPAA's privacy requirements, all Indiana EMS certificate holders risk being subject to fines and suspension or revocation of their Indiana Certificate for the "**Unauthorized disclosure of medical records or other confidential patient information**." Further, EMS services provided by or

See "HIPAA" page 5

"HIPAA" *from page 4*

under a contract with a public agency must make the following information available (See IC 16-31-2-11):

- The date and time of the request for ambulance services.
- The reason for the request for assistance.
- The time and nature of the response.
- The time of arrival at the scene.
- The time of departure from the scene.
- The name of the facility, if any, to which the patient was delivered.

Permitted Unauthorized Disclosures
THIS IS EXTREMELY IMPORTANT

These are the instances when a CE may disclose PHI without a patient's consent and NOT violate the Privacy Rule. These exemptions are extremely important to know. As always, though, if a patient consents to a disclosure, then a Covered Entity may disclose the consented-to PHI for the consented-to purpose.

These exemptions are found in ***45 CFR § 164.512*** Covered Entities ***MAY*** disclose PHI for:

- Treatment, Payment, and Operations.
- When Required by State or Federal Law.
- For Public Health Activities, which includes ***sending run report data to SEMA or NFIR.***
- Victims of Abuse, Neglect, or Domestic Violence.
- For Health Oversight Activities, which includes ***SEMA hearings.***
- For Judicial and Administrative Proceedings.
- For certain Law Enforcement purposes.
- For Births and Deaths.
- For Organ and Tissue Donation.
- For Certain Research Purposes.
- To Protect Public Safety.
- And For Certain Specialized Government Functions.

Your New Best Friend: Treatment, Payment, and Health Care Operations

Treatment, Payment, and Operations (TPO) disclosures are allowed without Patient authorization for:

- **Treatment -** giving PHI to other providers involved in treating the patient, such as a hospital or another EMS service involved in providing Patient Care.
- **Payment** - receiving PHI from other providers (such as a hospital) needed for billing for treatment you have previously provided to that patient. This includes filing claims, coordinating benefits, making eligibility inquiries, and even for taking collections activities.
- **Operations** - This includes disclosing PHI for Audit and Review, quality assessment, and medical or legal auditing.

Disclosures Required by Law

The Privacy Rule allows most disclosures of PHI statutorily required by Indiana law. The Minimum Necessary Rule, though, holds true for disclosures made under Indiana Law. This means that when disclosure of PHI is allowed under Indiana Law, disclose the *MINIMUM PHI NECESSARY* and only to the recipient specified in that Indiana law. For example, Indiana Law requires a practitioner* who initially treats an injury from fireworks or pyrotechnics to submit a report to the State Department of Health. As HIPAA exempts this and Indiana Law requires it, the State Department of Health MUST be given this report. Yet, the unauthorized release of the same information to local law enforcement, which is not required by either HIPAA or Indiana Law, would violate HIPAA.

*This code section defines a practitioner as anyone who holds an unlimited, limited, probationary, or temporary license, certificate, or registration.

Public Health Activities

This exemption allows disclosures of PHI to public health authorities authorized by State Law to receive that PHI and SPECIFICALLY ALLOWS sending run report data to SEMA or NFIRS. This also ALLOWS an EMS provider who has been exposed to blood or bodily fluids to request notification if the patient has a communicable disease. (See IC 16-41-10).

See "HIPAA" page 6

"HIPAA" *from page 5*

Victims of Abuse, Neglect, and Domestic Violence

This exemption allows the reporting of Abuse, Neglect, or Domestic Violence, when a State Law requires that reporting. Indiana Law requires a person who believes an "endangered adult" is a victim of battery, neglect, or exploitation to report this to Adult Protective Services or to law enforcement. Further, a person who believes that a child is a victim of abuse or neglect to immediately notify their boss and to immediately notify either local child protective services or local law enforcement.

Health Oversight Activities

This exemption allows the disclosure of PHI for SEMA investigations. It also allows disclosures to other supervising health entities. These include audits and investigations by supervising hospitals and/or supervising physicians, as well as Medicare audits and investigations.

Judicial and Administrative Proceedings

This exemption also allows disclosure of PHI for SEMA investigations. Disclosures under this exemption require an order from a Judge, an Administrative Law Judge, or a Grand Jury. These orders can be through a subpoena or a warrant. Yet, a subpoena or a warrant signed by an attorney or party to the litigation is not enough to require disclosure.

When Disclosure to Law Enforcement is allowed

A CE *may* disclose PHI to Law Enforcement when:

- Ordered by a court with a warrant or a subpoena signed by Judge, an Administrative Law Judge, or a Grand Jury, but not a warrant or subpoena signed by an attorney or a party to the litigation.
- When ordered through an administrative subpoena issued by an agency authorized to investigate the matter in question.
- And finally when the disclosure is required by state law. Disclosures required by state law are addressed in the note titled "Mandatory Disclosures of PHI Required by Indiana Law," which is available in the "HIPAA Presentation and Frequently Asked Questions" document available at: ***http://www.in.gov/sema/ems/***

Disclosure is allowed when needed to identify or locate a suspect, fugitive, missing person, or witness, the following PHI may be disclosed:

- name & address.
- date & place of birth.
- social security number.
- blood type.
- type of injury.
- date & time of treatment. (or death, if applicable)
- And these distinguishing characteristics: height, weight, gender, race, hair & eye color, scars, tattoos, and the presence or absence of facial hair.

Disclosure of PHI is permitted if the care recipient is a victim of crime AND:

- Is unable to consent; **AND**
- The officer states PHI needed to determine whether violation of law occurred by someone other than victim; **AND**
- The PHI is **NOT** intended to be used against the victim; **AND**
- Immediate Law Enforcement activity will be adversely affected by waiting until the victim can give consent; **AND**
- In your professional judgement you deem the disclosure is in the best interest of the victim.

This is a purposefully narrow exemption that further illustrates the role of care providers as patient advocates**.** This exemption only allows you, as a patient advocate, to make a disclosure that is "in the best interest of your patient."

Indiana law enforcement officers are statutorily required to gather the following information:

- Name and address of the owner and operator of each vehicle involved in the accident.
- License number and description of each vehicle
- Time and place the accident occurred.
- Name and address of each person injured or killed

See "HIPAA" page 7

"HIPAA" *from page 6*

- Name and address of each witness to the accident.

As State Law requires a law enforcement officer to collect the preceding information, disclosing the minimum necessary information should not violate the Privacy Rule. However, as EMS providers are patient advocates**,** they should always encourage law enforcement officers to gather information directly from the patient *when possible*, as opposed to from the EMS provider.

As this will be an ongoing issue, providers should begin work now with their attorneys, CEOs, provider hospitals, and local law enforcement to develop a policy for disclosing PHI to law enforcement.

Specialized Government Function

If any of the following uncommon disclosures arise, consider consulting with your attorney first:

- Military and Veteran Affairs.
- Department of Defense Activities.
- Required for national security.
- Required to protect the President or other national dignitaries.
- Security clearances.
- Inmates in governmental custody and others.

Other Allowed Disclosures

- Organ and Tissue Donation.
- For specific research purposes.
- To avert threats to safety: This exemption requires a good faith belief that the disclosure will:
- Prevent or lessen a serious & imminent threat to a person or to the public health; OR
- It will assist law enforcement *AFTER* an individual admits to involvement in a violent crime; OR
- You have reason to believe that the individual is a fugitive from the law. ●

GOT YOURS?

HOOSIER SAFETY
Summer 2003

Governor
Frank O'Bannon

Lt. Governor
Joseph E. Kernan

Executive Director
Patrick R. Ralston

Director, Public Information and Outreach
Alden Taylor

To submit information for publication, to be added to the mailing list or if you receive duplicate copies
● write to:
Bill Arend, Editor
Hoosier Safety
302 W. Washington Street
Room E208
Indianapolis, IN 46204-2760
● or call 317/232-6363
● or online at www.state.in.us/sema

Hoosier Safety is a quarterly publication of the Indiana State Emergency Management Agency and the Department of Fire and Building Services

REMINDER!!!

Don't Forget the 2003 Indiana Emergency Response Conference, September 19-21, at the Marriott Hotel Downtown, Indianapolis

West Valley radiation shipment safely on its way

In the late '60s a company near West Valley, New York proposed using spent fuel rods from nuclear reactors in a commercial venture. The project failed. The industrial site, along with the radioactive material, required clean up. During the past two and one half years, spent nuclear fuel rods had been scheduled to be transported through the central U.S. to east central Idaho for temporary storage until permanent storage at the Yucca Mountain, Nevada radioactive waste site is available. "The most significant fact is that this is the first time in the history of our nation that material with such a high level of radioactivity, has been moved this far," said Joseph Bell, SEMA's Director of Radiation Programs.

Safety of our citizens and the environment was, as usual, one of the primary concerns during this movement. As we stated in the Winter 2003 edition of Hoosier Safety ***(SHIPMENTS OF RADIOACTIVE WASTE PASS THROUGH INDIANA)***, there are very rigorous safety standards that these shipping containers must meet before being used. In the article we said ***"If you think the above testing is stringent, you should hear about the testing involving a locomotive running into a truck carrying one of these shipping containers, and a truck, with a container, moving at 60 MPH, running into a brick wall".*** These are the containers that received those additional safety tests!

Two shipping containers (see pictures) containing 125 fuel rods passed, without incident, through Indiana on a southwesterly route, from Allen County to Warren County, and on into Illinois, during the early morning hours of July 14, 2003. The well-coordinated project involving many state, federal, and tribal agencies along the entire route was also significant since the success of this shipment paves the way for the eventual transfer of some 77,000 tons of highly radioactive waste from 103 sites around the U.S. to the Yucca Mountain storage facility.

Above, personnel from the Indiana State Department of Health, Norfolk Southern Railroad Corporation, U.S. Departrment of Energy, and Illinois Department of Nuclear Safety conduct a "Radiation and Contamination Inspection" while the train is stopped at Peru, Indiana. The amount of radiation one receives during a dental x-ray is 20 times more than the radiation measured on the outside of these shipping containers.

John Ruyack (L) and Rex Bowser, Indoor and Radiological Health, Indiana State Department of Health, are responsible for monitoring radioactive material passing through the state of Indiana.

State Senator Marvin Riegsecker (R-Goshen), watches as the Second fuel rod container is readied for background radiation measurement.